Benjamin A. Schwartzman (SBN 02161)
BAILEY & GLASSER LLP
950 West Bannock Street, Suite 940
Boise, ID 83702
Telephone: (208) 342-4411
Facsimile: (208) 342-4455
bschwartzman@baileyglasser.com
(additional counsel listed on signature page)

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

TYLER BAKER, *individually, and on behalf of all others similarly situated,* Plaintiff, v. STANDARD INSURANCE COMPANY, Defendant.	**Case No. 3:23-cv-1407** **CLASS ACTION ALLEGATION COMPLAINT** **JURY TRIAL DEMANDED** **Action for Negligence, Negligence Per Se, Invasion of Privacy, Unjust Enrichment, Breach of Implied Contract, and Declaratory and Injunctive Relief**

CLASS ACTION COMPLAINT

Plaintiff Tyler Baker brings this Class Action Complaint against Standard Insurance Company ("Standard" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges—upon personal knowledge as to his own actions and his counsel's investigations and upon information and good faith belief as to all other matters—as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Defendant for its failure to properly secure and to safeguard personally identifiable information including, but not limited to, Plaintiff's

and Class Members' names, addresses, dates of birth and Social Security numbers (collectively, "Private Information" or "PII"). Defendant's severe failures have affected—and continue to affect—a class of over 300,000 people.

2. Standard provides group disability, statutory disability, life, dental, vision, critical illness, accident, hospital indemnity and absence management. During the course of its business operations, Defendant acquired, collected, utilized and derived a benefit from Plaintiff's and Class Members' Private Information.

3. Defendant owed and otherwise assumed statutory, regulatory and common law duties and obligations, including to keep Plaintiff's and Class Members' Private Information confidential, safe, secure and protected from the type of unauthorized access, disclosure and theft that occurred. As set forth herein, Defendant breached those duties and obligations.

4. On or about May 31, 2023, Defendant was notified by Pension Benefit Information, LLC ("PBI"), an entity that "provides audit and address research services," that some of Stanford's clients' Private Information was compromised due to a vulnerability in the widely used MOVEit file transfer software that PBI uses.

5. As set forth in a notice letter, dated as of September 6, 2023, received by Plaintiff,[1] Standard experienced a data breach between on or around May 29 to May 30, 2023, in which unauthorized third parties were able to access certain files on its network (the "Data Breach").[2]

[1] Upon information and good faith belief, Standard itself has taken no steps whatsoever to apprise the affected individuals that their Private Information has been compromised because of the Data Breach; for instance, there is no notice or other disclosure on its website regarding the Data Breach. *See* https://www.standard.com/ (last visited Sept. 23, 2023).

[2] *See* Notice Letter, attached as **Ex. A** hereto.

6. Upon information and belief, Defendant maintained the Private Information in a negligent manner. In particular, the Private Information was maintained on computer systems and networks that were in a condition vulnerable to cyberattack.

7. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant and therefore it was on notice that failing to take appropriate protective measures would expose and increase the risk that the Private Information could be compromised and stolen.[3]

8. This Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class Members.

9. While many details of the Data Breach remain in the exclusive control of Defendant, upon information and belief, Standard breached its duties and obligations by failing, in one or more of the following ways: (i) failing to design, implement, monitor and maintain reasonable network safeguards against foreseeable threats; (ii) failing to design, implement and maintain reasonable data retention policies; (iii) failing to adequately train staff on data security; (iv) failing to comply with industry-standard data security practices; (v) failing to warn Plaintiff and Class Members of Defendants' inadequate data security practices; (vi) failing to encrypt or adequately encrypt the Private Information; (vii) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (viii) failing to utilize widely available software able to detect and prevent this type of attack; (ix) failing to vet and/or adequately supervise its vendors to whom it had entrusted Private Information and (x) otherwise

[3] Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. The exposed Private Information of Plaintiff and Class Members can—and likely will—be sold repeatedly on the dark web.

failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

10. Plaintiff and Class Members now face a current and ongoing risk of identity theft, which is heightened here by the loss of Social Security numbers—the gold standard for identity thieves. Specifically, Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages, including: (i) invasion of privacy; (ii) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) the loss of benefit of the bargain (price premium damages); (viii) diminution of value of their Private Information; (ix) anxiety, annoyance and nuisance and (x) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

11. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, future costs of identity theft monitoring and injunctive relief including improvements to Defendant's data security systems and future annual audits. Accordingly, Plaintiff asserts claims, on behalf of himself and all others similarly situated, against Defendant for: (i) negligence, (ii) negligence per se, (iii) invasion of privacy; (iv) unjust enrichment, (v) breach of implied contract and (vii) declaratory judgment and injunctive relief.

PARTIES

12. Plaintiff Tyler Baker is an adult who, at all relevant times, was a resident and a citizen of the State of Vermont, residing in Underhill, Vermont, where he intends to remain indefinitely.

13. Plaintiff has been a policyholder of disability and/or accident insurance with Standard.

14. On or about September 20, 2023, Plaintiff received the Notice Letter notifying him that Defendant's network had been accessed and that his Private Information may have been involved in the Data Breach.

15. Defendant Standard Insurance Company is a holding company for businesses that provide insurance, retirement and investment products and services.[4] Standard provides group and individual disability insurance, group life, AD&D and dental insurance, retirement plans products and services, individual annuities to approximately 8.5 million people in the US.

16. Defendant is an Oregan corporation. Defendant's headquarters are located at 1100 SW Sixth Avenue in Portland, Oregon. Defendant is a subsidiary of StanCorp Financial Group, which is also headquartered in Portland, Oregon.

JURISDICTION & VENUE

17. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million, exclusive of interest and costs. Specifically,

[4] The Standard is a marketing name for Standard Insurance Company based in Portland, Oregon. Standard is licensed in all states except New York where it operates as The Standard Life Insurance Company of New York, based in White Plains, New York.

Class Members include policyholders who are citizens of numerous states other than Oregon, including, *inter alia*, Vermont. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

18. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

20. On or about May 31, 2023, Defendant became aware that its network may have been breached. Specifically, Progress Software, the provider of MOVEit Transfer software, disclosed that a vulnerability in their software had been exploited by an unauthorized third party.

21. PBI, which provides audit and address research services for insurance companies including Standard, utilized MOVEit in the course of its business operation to transfer files.

22. PBI did an investigation and discovered that cybercriminals had accessed a MOVEit server on May 29, 2023 and May 30, 2023, and downloaded data therefrom.[5]

23. The investigation revealed that the information compromised included the following types of information: name, social security number and date of birth.

B. Plaintiff Tyler Baker's Experience

24. Plaintiff was a client of Standard from approximately March of 2019 through approximately October of 2020.

[5] *See* Ex A, Notice.

25. As a requisite to receiving insurance services from Defendant, Plaintiff provided his Private Information to Defendant and trusted that the information would be safeguarded according to state and federal law. Upon receipt, Private Information was entered and stored on Defendant's network and systems.

26. Plaintiff is very careful about sharing his sensitive Private Information, and has never knowingly transmitted unencrypted sensitive Private Information

27. Plaintiff stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts. Had he known Defendant failed to follow basic industry security standards and failed to implement systems to protect his Private Information, he would not have provided that information to Defendant.

28. The Notice informed Plaintiff that Defendant's network had been accessed and his Private Information may have been involved in the Data Breach, which included his social security number, name and date of birth. The Notice directed Plaintiff to be vigilant and to take certain steps to protect his Private Information and otherwise mitigate his damages.[6]

29. As a result of the Data Breach, Plaintiff heeded that warning and spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Even with the best response, the harm caused to Plaintiff cannot be undone.

[6] *See id.*

30. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

31. Plaintiff also lost his benefit of the bargain by paying for insurance services that failed to provide the data security that was promised.

32. Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

33. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

34. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

35. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

C. The Data Breach Was Foreseeable

36. At all relevant times, Defendant knew or reasonably should have known of the importance of safeguarding the PII of Plaintiff and Class Members and the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

37. Defendant was or should have been fully aware of the unique type and the significant volume of data on its network, amounting to potentially millions of individuals'

detailed, personal information and thus the significant number of individuals who would be harmed by the exposure of sensitive data.

38. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[7]

39. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the insurance and financial services industry preceding the date of the breach.

40. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. Of the 1,862 recorded data breaches, 279 of them, or 14.98% were in the financial services industry.[8] The 279 reported breaches in 2021 exposed nearly 20 million sensitive records (19,978,108), compared to only 138 breaches that exposed nearly 2.7 million sensitive records (2,687,084) in 2020.

41. In light of recent high profile cybersecurity incidents at other insurance provider companies, including Bitmarck (300,000 policyholders, April 2023), Point32Health (2.5 million policyholders, April 2023), Latitude Financial (14 million customer records, March 2023), Capita (470,000 members, March 2023), and NationsBenefits (20 million members, January 2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

---

[7] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Sept. 23, 2023).

[8] *See* IAIS, Issues Paper on Cyber Risk to the Insurance Sector, https://www.iaisweb.org/uploads/2022/01/160812-Issues-Paper-on-Cyber-Risk-to-the-Insurance-Sector_final.pdf (last accessed Sept. 23, 2023).

42. Indeed, cyberattacks have become so notorious that the International Association of Insurance Supervisors had issued a warning to potential targets so they are aware of—and prepared for—a potential attack. As their 2016 Report explained, cyber risk presents a growing challenge for the insurance sector and one which, under the ICPs, supervisors are obliged to address. Insurers collect, store and manage substantial volumes of confidential personal and commercial information. Because of these reservoirs of data, insurers are prime targets for cyber criminals who seek information that later can be used for financial gain through extortion, identity theft or other criminal activities. In addition, because insurers are significant contributors to the global financial sector, interruptions of insurers' systems due to cybersecurity incidents may have far-reaching implications."[9]

43. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

D. The Financial Value of PII & PHI[10]

44. The PII of consumers remains of extremely high value to criminals, as evidenced by the prices offered through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at prices ranging from $40 to $200, and bank details have a price range of $50 to $200.[11]

---

[9] FBI, Secret Service Warn of Targeted, Law360 (Nov.18,2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware (last accessed Sept. 23, 2023).

[10] While the Notice does not state that Protected Health Information ("PHI") was involved in this breach, the presence of PHI on Defendant's network is relevant in assessing Defendant's duty of care in protecting Plaintiff's and Class Members' Private Information.

[11] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Sept. 23, 2023).

45. According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

46. The information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

47. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information…[is] worth more than 10x on the black market."[14]

48. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

49. The fraudulent activity resulting from the Data Breach may not come to light for years.

---

[12] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed Sept. 23, 2023).

[13] *In the Dark*, VPNOverview, 2019, available at https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Sept. 23, 2023).

[14] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Sept. 23, 2023).

50. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

51. There is also a robust legitimate market for the type of sensitive information at issue here. Marketing firms utilize personal information to target potential customers and an entire economy exists related to the value of personal data.

52. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

53. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

54. As such, future monitoring of financial and personal records is reasonable and necessary well beyond the one of protection offered by Defendant.

[15] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at*: https://www.gao.gov/assets/gao-07-737.pdf (last accessed Sept. 23, 2023).

E. Defendant Failed to Properly Protect Plaintiff's & Class Members' Private Information.

55. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiff and Class Members, as well as by properly vetting the cybersecurity practices of all entities to which it entrusted the Private Information. Moreover, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

56. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

57. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

58. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."

59. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

[16] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FED. TRADE COMM., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last accessed Sept. 23, 2023).

60. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

61. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[17]

62. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks…

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)…

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it….

[17] *Id.* at 3-4.

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic…[18]

63. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

[18] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last accessed Sept. 23, 2023).

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

64. Moreover, given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

65. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

F. Defendant Failed to Comply with FTC Guidelines

66. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

67. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly

[19] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www. (last accessed Sept. 23, 2023).

dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[20]

68. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

69. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

70. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

71. Orders resulting from these actions clarify the measures businesses take to meet their data security obligations.

72. Here, Defendant failed to properly implement basic data security practices.

[20] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Sept. 23, 2023).

73. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

74. Defendant was always fully aware of its obligation to protect the Private Information of Plaintiff and Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. Defendant Failed to Comply with Industry Standards

75. As shown above, experts studying cyber security routinely identify insurance providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

76. Several best practices have been identified that at a minimum should be implemented by insurance providers like Defendant, including, but not limited to educating all employees, strong passwords, multi-layer security, including firewalls, anti-virus and anti-malware software, encryption, making data unreadable without a key, multi-factor authentication, backup data and limiting which employees can access sensitive data.

77. Other best cybersecurity practices that are standard in the insurance industry include installing appropriate malware detection software, monitoring and limiting the network ports, protecting web browsers and email management systems, setting up network systems such as firewalls, switches and routers monitoring and protection of physical security systems, vetting and supervising any and all entities to which its clients' Private Information is entrusted and training staff regarding critical points.

78. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation

PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

79. The foregoing frameworks are existing and applicable industry standards in the insurance industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach. Upon information and good faith belief, Defendant failed to comply with one or more of the foregoing industry standards.

H. Defendant's Negligent Acts & Breaches.

80. Defendant participated and controlled the process of gathering the Private Information from Plaintiff and Class Members.

81. Defendant therefore assumed and otherwise owed duties and obligations to Plaintiff and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, testing of the data security policies and network systems.

82. Defendant breached these obligations to Plaintiff and Class Members and/or was otherwise negligent because it failed to properly implement data security systems and policies for its insurance providers network that would adequately safeguarded Plaintiff's and Class Members' Sensitive Information.

83. Upon information and good faith belief, Defendant's unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a) Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiff's and Class Members Private Information;

b) Failing to properly monitor its data security systems for data security vulnerabilities and risk;

c) Failing to test and assess the adequacy of its data security system;

d) Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e) Failing to put into develop and place uniform procedures and data security protections for its insurance network;

f) Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g) Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

h) Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

i) Failing to implement or update antivirus and malware protection software in need of security updating;

j) Failing to require encryption or adequate encryption on its data systems;

k) Otherwise negligently and unlawfully failing to safeguard Plaintiff's and Class Members' Private Information provided to Defendant, which in turn allowed cyberthieves to access its IT systems.

I. Plaintiff & Class Members Have Suffered Common Injuries & Damages.

84. As result of Defendant's ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

85. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of

pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

1. The Risk of Identity Theft to Plaintiff & Class Members Is Present & Ongoing.

86. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

87. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

88. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

89. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[21] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[22] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

90. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[23] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of

[21] *What Is the Dark Web?,* Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last accessed Sept. 23, 2023).

[22] *Id.*

[23] *What is the Dark Web*? – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last accessed Sept. 23, 2023).

birth, and medical information.[24] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[25]

91. Social Security numbers, for example, are among the worst kinds of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[26]
>
> What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

[24] *Id.*; What Is the Dark Web?, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/

[25] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web

[26] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Sept. 23, 2023).

92. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[27]

93. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

94. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[28]

95. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[29]

---

[27] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Sept. 23, 2023).

[28] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Sept. 23, 2023).

[29] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last accessed Sept. 23, 2023).

96. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[30] Defendant did not rapidly report to Plaintiff and the Class that their Private Information had been stolen.

97. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

98. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

99. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

100. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected

[30] *Id.*

by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[31]

101. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.

102. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[32]

103. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[33]

---

[31] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last accessed Sept. 23, 2023).

[32] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Sept. 23, 2023).

[33] *See e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last accessed Sept. 23, 2023).

104. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

2. Loss of Time to Mitigate the Risk of Identity Theft & Fraud.

105. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

106. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant's Website Notice instructs them, "Plac[e] credit freezes and/or fraud alerts with the three credit bureaus" and "add a password to your Genworth account to add a level of security in accessing your policy."

107. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity—which may take years to discover and detect—and filing police reports.

108. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office, who released a report in 2007 regarding data breaches ("GAO Report") in

which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[34]

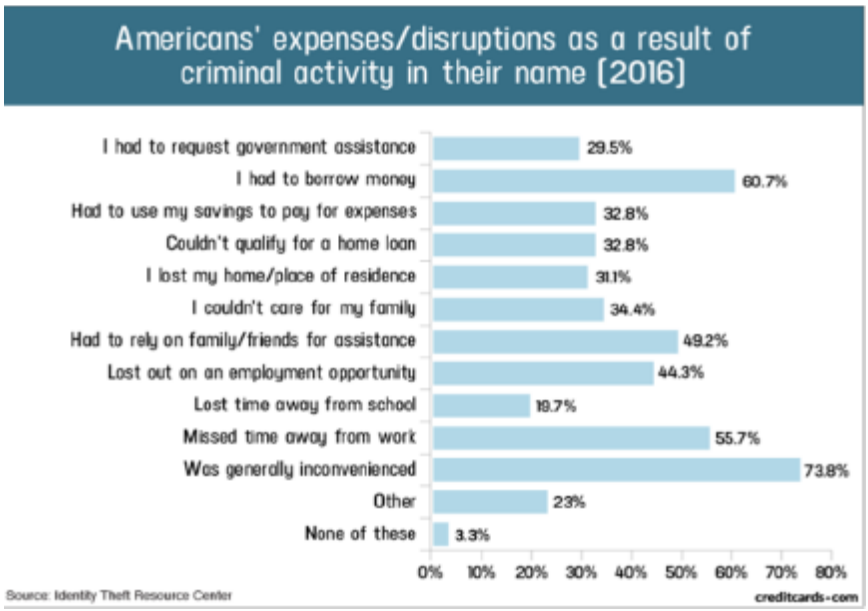
109. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

110. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[36]

[34] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[35] *See* Federal Trade Commission, IdentityTheft.com, https://www.identitytheft.gov/Steps (last accessed Sept. 23, 2023).

[36] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed Sept. 23, 2023).



111. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[37]

112. Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[38]

[37] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed Sept. 23, 2023).

[38] *See* https://www.identitytheft.gov/Steps (last accessed Sept. 23, 2023).

3. Diminution of Value of the Private Information.

113. PII is a valuable property right.[39] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

114. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

115. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[40]

116. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data was selling on the dark web for $50 and up.[41]

117. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[42] In fact, the data marketplace

[39] *See, e.g.*, John T. Soma, *et al.*, Corporate Privacy Trend: The "Value" of Personally Identifiable Information Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[40] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed Sept. 23, 2023).

[41] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed Sept. 23, 2023).

[42] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[43] [44] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[45]

118. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

119. To date, Defendant has done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant has not issued a notice of any kind, nor has it posted a notice on its website (the Notice that Plaintiff received regarding the Data Breach that compromised his and the Class Members' Private Information provided to Defendant was sent by PBI).[46]

---

[43] https://datacoup.com/

[44] https://digi.me/what-is-digime/

[45] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

[46] PBI has only offered one year of inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the foreseeable future. Defendant has not offered any other relief or protection. The one year of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. Defendant also places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

120. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the modus operandi of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – *e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

121. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

122. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[47] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

123. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

[47] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web*, New Report Finds, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed Sept. 23, 2023).

124. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

J. Injunctive Relief Is Necessary to Protect Against Future Data Breaches

125. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

CLASS ACTION ALLEGATIONS

126. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

127. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All persons residing in the United States whose PII was compromised in the Data Breach announced by PIB in or around September 2023, including all such individuals who were sent notice of the Data Breach (the "Nationwide Class").

128. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards,

sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

129. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

130. **Numerosity, Fed. R. Civ. P. 23(a)(1):** Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are 308,072 individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

131. **Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3):** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a) Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b) Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c) Whether Defendant had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d) Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e) Whether and when Defendant actually learned of the Data Breach;

f) Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g) Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

k) Whether Defendant violated the consumer protection statutes invoked herein;

l) Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m) Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n) Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

132. **Typicality, Fed. R. Civ. P. 23(a)(3):** Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

133. **Adequacy of Representation, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

134. **Predominance, Fed. R. Civ. P. 23(b)(3):** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single

action has important and desirable advantages of judicial economy. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

135. **Superiority, Fed. R. Civ. P. 23(b)(3):** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

136. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action

alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

137. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, uniform methods of data collection, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

138. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

139. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

140. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

141. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members and

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief because of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(*On Behalf of Plaintiff & the Nationwide Class*)

142. Plaintiff repeats and realleges each and every prior paragraph as if fully set forth herein.

143. Upon gaining access to the PII of Plaintiff and Class Members, Defendant owed to Plaintiff and Class Members a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties.

144. Further to this duty, Defendant was required to design, maintain, and test their security systems to ensure that these systems were reasonably secure and capable of protecting the PII of Plaintiff and the Class.

145. Defendant further owed to Plaintiff and Class Members a duty to vet and to adequately supervise all third parties to which it entrusted Plaintiffs' and Class Members' PII, as well as to implement systems and procedures that would detect a breach of their security systems in a timely manner and to timely act upon security alerts from such systems.

146. Defendant owed this duty to Plaintiff and Class Members because they are a well-defined, foreseeable, and probable class of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols.

147. Defendant actively solicited clients who entrusted Defendant with their PII when obtaining and using Defendant's services.

148. To facilitate these services, Defendant used, handled, gathered, and stored the PII of Plaintiff and Class Members. Attendant to Defendant's solicitation, use and storage, Thus, Defendant had a duty to act reasonably in protecting the PII of its policyholders.

149. The duty included obligations to take reasonable steps to prevent disclosure of the Private Information, and to safeguard the information from access, compromise, and theft.

150. Defendant's duties included the responsibility to design, implement and monitor data security systems, policies, and processes of third parties to whom it entrusted Plaintiffs' and Class Members' PII to protect against reasonably foreseeable data breaches such as this Data Breach.

151. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure

that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the Private Information.

152. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its clients, which is recognized by laws and regulations including, but not limited to, under Section 5 of the FTCA, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

153. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information that it either acquires, maintains, or stores.

154. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information, as alleged and discussed above.

155. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the insurance industry.

156. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

157. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and they sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating

the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

158. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

159. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

160. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(*On Behalf of Plaintiff the Nationwide Class*)

161. Plaintiff repeats and realleges each and every prior paragraph as if fully set forth herein.

162. Pursuant to Federal Trade Commission, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

163. Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

164. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards.

165. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Class Members due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

166. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se.*

167. Plaintiff and Class Member are within the class of persons that the FTC Act was intended to protect.

168. The harm that occurred because of the Data Breach is the type of harm the FTC Act was intended to guard against.

169. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

170. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

171. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

172. Defendant owed Plaintiff and Class Members a duty to notify them within a reasonable time frame of any breach to their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of Defendant's Data Breach.

173. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendant actively sought and obtained the PII of Plaintiff and Class Members.

174. Defendant breached their duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. And but for Defendant's negligence, Plaintiff and Class Members would not have been injured. The specific negligent acts

and omissions committed by Defendant include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to comply with—and thus violating—FTCA and its regulations;

c. Failing to adequately monitor the security of its networks and systems;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

f. Failing to detect in a timely manner that Class Members' PII had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

175. Plaintiff seek to remedy these harms on behalf of himself and all similarly situated and "impacted" individuals whose Private Information was accessed during the Data Breach, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) anxiety, annoyance and nuisance, (i) nominal damages, and (j) the future costs of identity theft monitoring.

176. Simply put, Defendant's negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their

bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

177. Moreover, Plaintiff's and Class Members' Private Information remains at risk, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

178. Plaintiff and the Class Members are entitled to compensatory and consequential damages suffered because of the data breach.

179. Therefore, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity theft monitoring to all Class Members.

COUNT III
INVASION OF PRIVACY
(*On Behalf of Plaintiff & the Nationwide Class*)

180. Plaintiff repeats and realleges each and every prior paragraph as if fully set forth herein.

181. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

182. As a result of Defendant's conduct, publicity was given to Plaintiff's and Class Members' Private Information, which necessarily includes matters concerning their private life such as PII.

183. A reasonable person of ordinary sensibilities would consider the publication of Plaintiff's and Class Members' Private Information to be highly offensive.

184. Plaintiff's and Class Members' Private Information is not of legitimate public concern and should remain private.

185. As a direct and proximate result of Defendant's public disclosure of private facts, Plaintiff and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

186. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

187. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(*On Behalf of Plaintiff & the Nationwide Class*)

188. Plaintiff repeats and realleges each and every prior paragraph as if fully set forth herein.

189. This count is pleaded in the alternative to Count V, Breach of Implied Contract.

190. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying money for insurance services that relied on Defendant to render certain services, a portion of which was intended to have been used by Defendant for data security measures to secure Plaintiff and Class Members' PII.

191. Plaintiff and Class Members further conferred a benefit on Defendant by entrusting their PII to Defendant and its customers from which Defendant derived profits.

192. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide adequate security.

193. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

194. Defendant acquired the monetary benefit, PII, through inequitable means in that Defendant failed to disclose the inadequate security practices, previously alleged, and failed to

maintain adequate data security.

195. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to give their money—or disclosed their data—to Defendant or Defendant's customers.

196. Plaintiff and Class Members have no adequate remedy at law.

197. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their PII is used; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (6) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of Defendant's Data Breach.

198. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered—and will continue to suffer—other forms of injury and/or harm.

199. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from Plaintiff and Class Members.

COUNT V
BREACH OF IMPLIED CONTRACT
(*On Behalf of Plaintiff & the Nationwide Class*)

200. Plaintiff repeats and realleges each and every prior paragraph as if fully set forth herein.

201. This count is pleaded in the alternative to Count IV Unjust Enrichment.

202. Plaintiff's and Class Members' PII was provided to Defendant in exchange for the goods and the services that Defendant provided to Plaintiff and Class Members.

203. Plaintiff and Class Members agreed to pay Defendant for such goods and services.

204. Defendant and the Plaintiff and Class Members entered into these implied contracts which included an understanding that Defendant would provide adequate data security. This understanding was separate and apart from any express contracts concerning the security of Plaintiff's and Class Members' PII, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiff's and Class Members' PII.

205. Defendant had an implied duty of good faith to ensure that the PII of Plaintiff and Class Members was only used in accordance with the parties' contractual obligations.

206. Defendant was, therefore, required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and to comply with industry standards and applicable laws and regulations for the security of this information.

207. Under these implied contracts which included data security services and obligations, Defendant was further obligated to provide Plaintiff and all Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

208. However, Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII and timely detect the Data Breach, resulting in the harms now alleged herein.

209. Indeed, Defendant further breached these implied contracts by providing untimely notification to Plaintiff and Class Members who are already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

210. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

211. As a result of Defendant's conduct, Plaintiff and Class Members did not receive the full benefit of their bargain with Defendant.

212. Had Defendant disclosed that its data security was inadequate, neither the Plaintiff nor Class Members, nor any reasonable person would have entered into such contracts with Defendant.

213. As a result of the Data Breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain at present risk of suffering additional damages.

214. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

215. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT VI
DECLARATORY AND INJUNCTIVE RELIEF
(*On Behalf of Plaintiff & the Nationwide Class)*

216. Plaintiff and the Class repeat and re-allege paragraphs 1-141 of the Complaint as if fully set forth herein.

217. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

218. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

219. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

220. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect employee and patient Private Information.

221. Defendant still possesses the Private Information of Plaintiff and the Class.

222. To Plaintiff's knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information, beyond the vague

claim in the Data Breach Letter that it is "making [its] computer systems even stronger than before because [it does] not want this to happen again."

223. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

224. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Standard. The risk of another such breach is real, immediate, and substantial.

225. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

226. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

227. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Standard, Plaintiff and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

228. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Standard, thus eliminating the additional injuries that would result to Plaintiff and Class.

229. Plaintiff and Class Members, therefore, seek a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Tyler Baker, on behalf of himself and Class Members, respectfully requests judgment in his favor and against Defendant Standard Insurance Company as follows:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: September 27, 2023

Respectfully Submitted,

BAILEY & GLASSER LLP

/s/ Benjamin A. Schwartzman

Benjamin A. Schwartzman (SBN 02161)
950 West Bannock Street, Suite 940
Boise, ID 83702
Telephone: (208) 342-4411
Facsimile: (208) 342-4455
bschwartzman@baileyglasser.com

By: */s/ David S. Almeida*
David S. Almeida*
Elena A. Belov*
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

By: */s/ Brandon M. Wise*
Brandon M. Wise*
PEIFFER WOLF CARR KANE CONWAY & WISE, LLP
818 Lafayette Ave., Floor 2
St. Louis, MO 63104
Ph: (314) 833-4825
bwise@peifferwolf.com

By: */s/ Andrew R. Tate*
Andrew R. Tate*
PEIFFER WOLF CARR KANE CONWAY & WISE, LLP
235 Peachtree Street NE, Suite 400
Atlanta, GA 30303
Ph: (404) 282-4806
atate@peifferwolf.com

**Pro Hac Vice* admission to be sought

COUNSEL FOR PLAINTIFF & CLASS MEMBERS